FIA/DEEP-09-001-S
ATTACHMENT S

DHR INFORMATION SYSTEMS SECURITY HANDBOOK

INFORMATION SYSTEMS SECURITY HANDBOOK

State of Maryland
Department of Human Resources
Office of Technology for Human Services
Office of Information Management
Data Security Division

General Policy Statement

Information is a State of Maryland (SOM) asset requiring protection commensurate with its value. Measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional, as well as to assure its authenticity, integrity, availability, and confidentiality.

Scope

The controls in this handbook are the minimum requirements for providing a secure environment for utilizing, developing, implementing, and maintaining automated systems in the Department of Human Resources.

These controls apply to all Department of Human Resource entities, agents, employees, contractors, or vendors involved in the the utilization, development, implementation, and maintenance of information systems.

Any exception to these controls should be reviewed by the Data Security Division and receive their documented approval.

Compliance

All Department of Human Resource employees, agents, contractors, and vendors are responsible for understanding and complying with these controls. This would include building and configuring systems in accordance with these policies. Non-compliant situations will be brought to the attention of management for appropriate action. Depending on the severity of the occurrence, employees who violate these policies may receive loss of network connectivity, disciplinary action, up to and including immediate dismissal, and/or criminal prosecution.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure either compliance with State of Maryland policies or that a level of control is provided which is equivalent to State of Maryland policies. This should be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

All necessary exceptions to this policy must be clearly documented and approved by the agency head and the Data Security Division.

Confidentiality

All Department of Human Resource employees, agents, contractors, and vendors are responsible for keeping confidential all data contained in the DHR Automated Systems to which they are granted access. Authority: Article 88A, §5 and 6; State Government Article, §10-611 et seq. Article 41, Title 6; Annotated Code of Maryland. 07.01.07.00. 5 and 6; State Government Article, §10-611 et seq.

Security Access Controls

All security access controls used today depends on a profile being set up to protect a resource, with logonids being allowed or disallowed connection to utilize the protected resource. Access controls do not normally allow an inquiry on an individual as to what access they have. An inquiry would query protected resources to see if the logonid assigned to that individual is connected or not, and to what level.

Security Access Control:

RACF at IBM/GS Data Center
ACF2 at ADC & MDOT Data Center

Once access to the resources at the various data centers is established via VTAM, then access is authenticated to the individual resources.

These resources are generally data-sets, data tables, terminal I/O, system applications, and CICS transactions that allow communication to customer applications.

Computer Security Awareness

☆ Password protect your workstation with a "screensaver" password, set to automatically lock your system after no more than two minutes of non-activity.

☆ Log out of any main-frame applications, including those that use client-server or web based access, when leaving your workstation unattended.

☆ Select a "strong" set of passwords, don't use the same one for all access, and never share this information with anyone. A "strong" password will contain a mixture of alpha, numeric, and special characters. Always use a password that does not appear in a dictionary.

☆ Make sure that your workstation is protected by an Agency supplied or approved anti-virus software.

☆ Never access any unknown, unsolicited, or suspicious e-mail attachment. Even if you know the sender, verify that they did, in fact, send it to you.

☆ Always back-up the data that you have on your workstation hard drive.

☆ Use your State furnished workstation for work related activities only.

☆ Load no unauthorized or illegal software on your State furnished workstation.

☆ Keep all sensitive client and co-worker information confidential. This includes case information, Social Security Numbers, logonids, and passwords.

Access Notification

All Automated System access should be deemed as covered by the following:

WARNING! THIS SYSTEM MAY CONTAIN GOVERNMENT INFORMATION, WHICH IS RESTRICTED TO AUTHORIZED USERS ONLY. UNAUTHORIZED ACCESS, USE, MISUSE, OR MODIFICATION OF THIS COMPUTER SYSTEM OR OF THE DATA CONTAINED HEREIN OR IN TRANSIT TO/FROM THIS SYSTEM CONSTITUTES A VIOLATION OF ARTICLE 27 §§ 45A AND 146 OF THE ANNOTATED CODE OF MARYLAND, TITLE 18, USC, § 1030, AND MAY SUBJECT THE INDIVIDUAL TO CRIMINAL AND CIVIL PENALTIES PURSUANT TO TITLE 26, USC, §§ 7213(A), 7213A, AND 7431. THIS SYSTEM AND EQUIPMENT ARE SUBJECT TO MONITORING TO ENSURE PROPER PERFORMANCE OF APPLICABLE SECURITY FEATURES OR PROCEDURES. SUCH MONITORING MAY RESULT IN THE ACQUISITION, RECORDING AND ANALYSIS OF ALL DATA BEING COMMUNICATED, TRANSMITTED, PROCESSED OR STORED IN THIS SYSTEM BY A USER. IF MONITORING REVEALS POSSIBLE EVIDENCE OF CRIMINAL ACTIVITY, SUCH EVIDENCE MAY BE PROVIDED TO LAW ENFORCEMENT PERSONNEL. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

This is to considered the stated and implied agreement excepted by all DHR or DHR approved users of the Automated Systems of the State of Maryland.

Data Storage and Processing Facility

The DHR utilizes the International Business Machine/Global Systems (IBM/GS) Data Center for all of its applications. The Annapolis Data Center (ADC) is utilized for most other agency applications, such as MABS, MMIS, ASM, etc. The MVA access is utilized at the Maryland Department of Transportation Data Center (MDOTDC). IBM/GS uses the Resources Access Control Facility (RACF) as its' security software and the ADC as well as the MDOTDC uses the Access Control Facility 2 (ACF2) as its' security software.

Both of these security software packages allow a "controlled sharing of data" by permitting access only when explicit action is taken by the data owner and by a security officer who authorizes it. Authorization is permitted by the use of logonids and passwords.

Security Personnel Designation

In order for an adequate level of security to exist in the DHR application systems an agency data security structure has been developed. The access procedure begins with the DHR employee's immediate supervisors that are requesting security access and ends with the DHR Security Officers of the OIM/DSD. This structure is intended to provide a systematic means for staff to protect data and to gain the proper level of access to DHR's automated systems.

Security Monitor Appointment

In order to delegate the authority of requesting access to the DHR Automated Systems for their staff, the appropriate Appointing Authority will appoint a Primary and at least one Secondary Security Monitor.

The process consists of the Appointing Authority signing to authorize a properly completed DHR/OIM 671 form. This form must contain among other information, the fax number, e-mail address, and the signature of the Security Monitor. This form is also to be used to appoint Network Administrators to interface with the DHR WAN/LAN.

The functions of these Security Monitors are important and necessary for the secure utilization of the DHR Automated Systems. They are responsible for requesting access for the staff they support, acting with the authority of the Appointing Authority.

While they act with the authority of the Appointing Authority in requesting access, if the DSD rejects the request, the appropriate Appointing Authority must sign off on the request and provide additional justification as to why the exception is necessary, should they chose to resubmit.

Security Monitor's Responsibilities:

☆ To expeditiously review forms (for accuracy and completeness), to sign and forward the appropriate security transaction form(s) to the DSD whenever an employee needs to be added to or deleted from a system; have his/her system access level modified; or have his/her name changed. Security monitors are the only staff members authorized to forward Security Access Forms(s) to the DSD or to inquire about their status.

☆ To notify the supervisor and/or the end user of the status of his/her security access request.

☆ To keep copies of all forms sent to the DSD as well as all rejected or completed forms returned.

☆ To report all access problems to the DHR System Support. Security Monitors are the only staff members authorized to call the DHR System Support Center concerning system access problems.

☆ To remind supervisors to forward all security access transaction forms to the Security Monitors as soon as an employee enters or leaves a unit or local department.

☆ To remind supervisors that it is their responsibility to monitor an employee's security access levels for appropriateness to their job responsibilities and to take corrective action when necessary.

☆ To communicate as needed or at least annually to supervisors, staff, and others the requirement that DHR's data is to be kept confidential and that the passwords are to be kept a secret.

☆ To serve as a liaison between the Local Department and the DSD.

☆ To review and disseminate all Data Security material. Primary Security Monitors must distribute all Security Alerts and other security related information to secondary Security Monitors.

☆ To ensure that the current versions of security access forms are being utilized.

☆ To ensure adherence to all controls concerning security access requests.

DHR Logonid Deletion Policies

RACF logonids will be deleted from DHR's systems after ninety (90) days of non-use. MVA logonids will be deleted from their system after sixty (60) days of non-use. ADC logonids will be deleted from their system after ninety (90) days of non-use. EBTS logonids will be suspended from their system after thirty (30) days of non-use, revoked after sixty (60) days, and deleted after ninety (90) days. A user can avoid being deleted or suspended from these systems by simply logging in and out within the time lines set.

Password Information

Password Rules:

☆ Must be at least six (6), but no more than eight (8) positions in length.

☆ Must contain an alphabetic character in the first and last positions.

☆ Must contain at least one (1) numeric character.

☆ Must not contain your logonid as part of your password.

☆ Must not contain more than two identical consecutive characters.

☆ Must not contain more than three (3) identical, consecutive characters in the same position as in your previous password.

☆ Must be changed at least once every ninety (90) days.

☆ Old passwords may not be used again for thirteen (13) consecutive password changes.

☆ Access privileges will be suspended after three (3) unsuccessful attempts to sign-on.

Examples

☆	Examples of valid passwords:	ABC1ABC	
☆	Examples of invalid passwords:	A011795B	
		ABC12	(Rule #1,2)
		123456	(Rule # 2)
		AAA234B	(Rule # 6)
		ABCDEF	(Rule # 3)
		USERID5X	(Rule # 4)

DHR/OIM Security Access Forms

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
LOGONID REQUEST

ACTION: ADD □ UPDATE □ DELETE □ DATE OF REQUEST: _____/_____/_____ CURRENT LOGONID: __________

EMPLOYEE NAME (PRINT): _______________ (FIRST) _______________ (LAST) LDSS: __________

PHONE: (_____) _____-_____ JOB CLASSIFICATION: _______________ DISTRICT: __________

LOCATION CODE: ____ STATE EMPLOYEE: YES □ NO □ IF NO EXPLAIN: _______________

OTHER ACTION: □ (SPECIFY): _______________

INQUIRY ACCESS MENU

AIMS □ AMF □ MABS □ MMIS □ SVES □ SOLQ □ (IF CHECKED A SIGNED AND WITNESSED DHR/HRDT 73 MUST BE ON FILE WITH HRDT)

FACTS: A □ B □ C □ (SELECT ONE ONLY) TERM ID (4 CHAR): _____ _____ _____ _____ _____ _____

DBM PERSONNEL □ TERM ID (4 CHAR): _____ _____ _____ _____ PRINTER ID (4 CHAR): _____ _____ _____

DHR PERSONNEL □ TERM ID (4 CHAR): _____ _____ _____ _____ PRINTER ID (4 CHAR): _____ _____ _____

OTHER ACCESS REQUIRED

CARES: □ (IF CHECKED ATTACH A COMPLETED DHR/OIM 672 CARES ACCESS REQUEST)

CSES: □ (IF CHECKED ATTACH A COMPLETED DHR/OIM 672b CSES ACCESS REQUEST)

MVA: □ (IF CHECKED ATTACH COMPLETED MVA ISC-OOS-011 & MVA OIR-ISS-10 FORMS)

CCAMIS: □ (IF CHECKED ATTACH A COMPLETED DHR/OIM 673 CCAMIS LOGONID REQUEST)

EBTS: □ (IF CHECKED ATTACH A COMPLETED DHR/OIM 674 EBTS LOGONID REQUEST)

ASM: □ (IF CHECKED ATTACH OR SUBMIT TO ASM STAFF COMPLETED ASM REQUEST)

MDChessie: □ (DO NOT USE)

OR DESCRIBE

____

____

____

SUPERVISOR

SIGNATURE: ____________________ DATE: _____/_____/_____

NAME (PRINT): ____________________ PHONE: (_____) _____-_____

SECURITY MONITOR

SIGNATURE: ____________________ DATE: _____/_____/_____ FAX: (_____) _____-_____

NAME (PRINT): ____________________ PHONE: (_____) _____-_____

DHR SECURITY OFFICER USE ONLY

ACTION TAKEN: ADDED □ UPDATED □ DELETED □ REJECTED □ DATE SENT TO MVA/CCAMIS/ETC: _____/_____/_____

REJECTION REASON: ____________________ LOGONID ASSIGNED: __________

SIGNATURE: ____________________ DATE: _____/_____/_____ CNTL: __________

DHR/OIM 670 (02/03) RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS.

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
SECURITY MONITOR SIGNATURE VERIFICATION

ACTION: ADD □ UPDATE □ DELETE □ DATE OF REQUEST : _____/_____/_____

LEVEL: PRIMARY □ SECONDARY □ PLATFORM: MAINFRAME □ NETWORK □

LOCATION:

LDSS/AGENCY ____

DISTRICT/LOCAL OFFICE ______________________________ LOCATION CODE: __ __

SECURITY MONITOR

EMPLOYEE NAME (PRINT): ________________ (FIRST) ________________ (LAST) DATE: _____/_____/_____

SIGNATURE: ____________________________ PHONE: (_____) _____-_____

FAX: (_____) _____-_____ E-MAIL: ____________________________

ADDRESS: ____

CITY, STATE, ZIP: ____________________________________

JOB CLASSIFICATION: __________________________________

JOB TITLE: ____

STATE EMPLOYEE: YES □ NO □ IF NO EXPLAIN: ____________________________

APPOINTING AUTHORITY

TITLE: ____

NAME (PRINT): ________________ (FIRST) ________________ (LAST) DATE: _____/_____/_____

SIGNATURE: ____________________________ PHONE: (_____) _____-_____

FAX: (_____) _____-_____ E-MAIL: ____________________________

ADDRESS: ____

CITY, STATE, ZIP: ____________________________________

DHR SECURITY OFFICER USE ONLY

ACTION TAKEN: ADDED □ UPDATED □ DELETED □ REJECTED □

REJECTION REASON: __________________________________

SIGNATURE: ____________________________ DATE: _____/_____/_____

RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES

CARES ACCESS REQUEST

ACTION: ADD □ UPDATE □ SUSPEND □ DATE OF REQUEST: ____/____/____ CURRENT LOGONID: ________

EMPLOYEE NAME (PRINT): ______________ (FIRST) ______________ (LAST) LDSS: ________

PHONE: (____) ____-______ JOB CLASSIFICATION: ______________ DISTRICT: ________

LOCATION CODE: ____ STATE EMPLOYEE: YES □ NO □ IF NO EXPLAIN: ______________

NOTICE NAME (PRINT): ______________ USER'S SYSTEM: CARES □ SERVICES □

NON PRODUCTION CICS REGION(S): ______________

CARES

WORKER TYPE ____ UNIT TYPE ______ UNIT NUMBER ______ DISTRICT OFFICE ______ LDSS ACCESS __

SERVICES

WORKER TYPE __ FACTS WORKER TYPE __ WORKER ID ______

UNIT TYPE ____ UNIT NUMBER ____ DISTRICT OFFICE ______

SECURED TASKS

DELETE SECURED TASKS: ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___
___ , ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___
___ , ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___

ADD SECURED TASKS: ___ , ___ , ___ , ___ , ___ , ___ , ___ , ___
___ , ___ , ___ , ___ , ___ , ___ , ___ , ___

SUPERVISOR

SIGNATURE: ______________ DATE: ____/____/____

NAME (PRINT): ______________ PHONE: (____) ____-______

SECURITY MONITOR

SIGNATURE: ______________ DATE: ____/____/____ FAX: (____) ____-______

NAME (PRINT): ______________ PHONE: (____) ____-______

DHR SECURITY OFFICER USE ONLY

ACTION TAKEN: ADDED □ UPDATED □ DELETED □ REJECTED □

REJECTION REASON: ______________

SIGNATURE: ______________ DATE: ____/____/____ CNTL: ________

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES

CSES ACCESS REQUEST

ACTION: ADD □ UPDATE □ DELETE □ DATE OF REQUEST: ____/____/____ CURRENT LOGONID: ____________

TEMPORARY UPDATE □ BEGIN DATE: ____/____/____ END DATE: ____/____/____

EMPLOYEE NAME (PRINT): ____________ (FIRST) ____________ (LAST) LDSS: ____________

PHONE: (______) ______-________ JOB CLASSIFICATION: ____________ DISTRICT: ____________

LOCATION CODE: _____ STATE EMPLOYEE: YES □ NO □ IF NO EXPLAIN: ____________

NON PRODUCTION CICS REGION(S): ____________

EXISTING ROLE(S): __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __
__ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __

DELETE ROLE(S): __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __
__ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __

ADD ROLE(S): __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __
__ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __, __ __

CARES ACCESS

COUNTY ___ AGENCY LEVEL ___ SECURITY LEVEL ___ UNIT TYPE 60 UNIT NUMBER 60 DISTRICT OFFICE 002

JUSTIFICATION

____

____

____

____________ LOCAL DIRECTOR ____________ EXECUTIVE DIRECTOR, CSEA

SUPERVISOR

SIGNATURE: ____________ DATE: ____/____/____

NAME (PRINT): ____________ PHONE: (______) ______-________

SECURITY MONITOR

SIGNATURE: ____________ DATE: ____/____/____ FAX: (______) ______-________

NAME (PRINT): ____________ PHONE: (______) ______-________

DHR SECURITY OFFICER USE ONLY

ACTION TAKEN: ADDED □ UPDATED □ DELETED □ REJECTED □

REJECTION REASON: ____________

SIGNATURE: ____________ DATE: ____/____/____ CNTL: ____________

DHR/OIM Security Access Form Procedures

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
PROCEDURE FOR COMPLETING DATA SECURITY ACCESS FORMS

FORM NUMBER:	**DHR/OIM 670 (02/03)**	**ISSUED: 14FEB03**	**REVISED:**	**PAGE 1 OF 3**

USAGE: Used for the adding, updating, and deleting of mainframe DHR logon identifications (logonids).

PROCEDURE: The Supervisor completes and signs the DHR/OIM 670 and submits it to the local security monitor. The local security monitor authorizes the request(s) and submits the signed form(s) to the DHR Data Security Division.

INSTRUCTIONS FOR COMPLETING THE FORM:

ACTION: .... Check one box per request:

ADD - to establish a new logonid
UPDATE - to change the employee's access privileges or to modify their information
DELETE - to remove the logonid from ALL system access

DATE OF REQUEST: .... Enter the current date.

CURRENT LOGONID: .... Enter the employee's logonid. (THIS IS REQUIRED FOR UPDATE and DELETE).

EMPLOYEE NAME (PRINT): .... Enter the name of the employee.

(FIRST) - enter first name here
(LAST) - enter last name here

NOTE: If a name change is requested, indicate this in the OTHER ACTION section along with the current name.

LDSS: .... Enter the LDSS or agency location name. Refer to Appendix B.

PHONE: .... Enter the area code and telephone number of the employee.

JOB CLASSIFICATION: .... Enter the job classification of the employee. (THIS IS REQUIRED FOR ADD and UPDATE)

DISTRICT: .... Enter the local department's district location name, if applicable.

LOCATION CODE: .... Refer to Appendix B. (2 DIGIT CODE ONLY).

STATE EMPLOYEE: .... Check the appropriate box.

IF NO EXPLAIN: .... If the logonid request is not for a state employee supply justification for the logonid.

OTHER ACTION: .... Specify special requests that are not provided for on the logonid request form.

INQUIRY ACCESS MENU

AIMS: .... Check if applicable. Update capabilities are no longer available.

AMF: .... Check if applicable. Update capabilities are available only for DHR Central Staff.

MABS: .... Check if applicable.

MMIS: .... Check if applicable.

SVES: .... Check if applicable.

SOLQ .... Check if applicable. If checked a signed and witnessed DHR/HRDT 73 must be on file with the HRDT, or attached.

INSTRUCTIONS FOR COMPLETING THE FORM (CONTINUED) :

FACTS: .... Check either A, B, or C, refer to Appendix I. Update capabilities are no longer available.

TERM ID: .... Enter terminal identification code(s). (FOUR CHARACTER CODES ONLY).

DBM PERSONNEL: .... Check if applicable.

TERM ID: .... Enter terminal identification code(s). (FOUR CHARACTER CODES ONLY).

PRINTER ID: .... Enter printer identification code(s). (FOUR CHARACTER CODES ONLY).

DHR PERSONNEL: .... Check if applicable.

TERM ID: .... Enter terminal identification code(s). (FOUR CHARACTER CODES ONLY).

PRINTER ID: .... Enter printer identification code(s). (FOUR CHARACTER CODES ONLY).

OTHER ACCESS REQUIRED

CARES: .... Check box and attach a properly completed and signed DHR/OIM 672 form This is necessary for initial requests. Subsequent changes may be submitted on a DHR/OIM 672 form alone.

CSES: .... Check box and attach a properly completed and signed DHR/OIM 672b form This is necessary for initial requests. Subsequent changes may be submitted on a DHR/OIM 672b form alone.

MVA: .... Check box and attach properly completed and signed form(s). This request must always be attached to a DHR/OIM 670 form.

CCAMIS: .... Check box and attach a properly completed and signed DHR/OIM 673 form. This is needed for the initial request. Subsequent changes may be submitted on a DHR/OIM 673 form alone.

EBTS: .... Check box and attach a properly completed and signed DHR/OIM 674 form. This request must always be attached to a DHR/OIM 670 form.

ASM: .... Check box for ASM (FMIS) and attach, or submit to ASM staff, a properly completed and signed ASM request form.

MD Chessie: .... DO NOT USE THIS ACCESS

OR DESCRIBE

Print description of special (not otherwise noted on this form) access.

SUPERVISOR

SIGNATURE .... Enter the signature of the supervisor of the employee noted.

DATE: .... Enter the date the above signature was added.

NAME (PRINT): .... Enter the first and last name of the supervisor of the employee noted.

PHONE: .... Enter the area code and telephone number of the security monitor.

INSTRUCTIONS FOR COMPLETING THE FORM (CONTINUED) :

SECURITY MONITOR

SIGNATURE .... Enter the signature of the security monitor.

DATE: .... Enter the date the above signature was added.

FAX: .... Enter the area code and facsimile number of the security monitor.

NAME (PRINT): .... Enter the first and last name of the security monitor.

PHONE: .... Enter the area code and telephone number of the security monitor.

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
PROCEDURE FOR COMPLETING DATA SECURITY ACCESS FORMS

FORM NUMBER: DHR/OIM 671 (02/03) **ISSUED:** 14FEB03 **REVISED:** **PAGE 1 OF 2**

USAGE: Used to verify the signatures of appointed security monitors who submit DHR/OIM security access forms.

PROCEDURE: The appointing authority (Local Director DSS, Administration's Executive Director, etc.) appoints one or more staff as security monitors. The appointing authority completes and signs a DHR/OIM 671 for each monitor selected and submits the completed form to the DHR Data Security Division.

NOTE: A properly completed form is required to appoint, delete, or to change level, address, phone, or fax.

INSTRUCTIONS FOR COMPLETING THE FORM:

ACTION: .... Check one box per request:

- ADD - to establish a new security monitor for a certain location.
- UPDATE - to modify the security monitor's information or to change the security monitor's status as a primary or secondary
- DELETE - to remove a security monitor

DATE OF REQUEST: .... Enter the current date.

LEVEL: .... Check one box per request:

- PRIMARY - Only one allowed per jurisdiction/modal/office. This is the main security contact for that jurisdiction/modal/office.
- SECONDARY - At least one recommended.

PLATFORM: .... Check one or both boxes:

- MAINFRAME - Duties performed as a security monitor for State and DHR Automated Systems
- NETWORK -Duties performed as a DHR WAN / LAN administrator

LOCATION

LDSS/AGENCY .... Enter the LDSS or agency location name. Refer to Appendix B.

DISTRICT/LOCAL OFFICE ..... Enter the district or local office name

LOCATION CODE: .... Refer to Appendix B. (2 DIGIT CODE ONLY).

INSTRUCTIONS FOR COMPLETING THE FORM (CONTINUED) :

SECURITY MONITOR

EMPLOYEE NAME (PRINT): . . . Enter the name of the employee.

(FIRST) - enter first name here
(LAST) - enter last name here

DATE: . . . . Enter the date the signature below was added.

SIGNATURE . . . . Enter the signature of the security monitor.

PHONE . . . . Enter the area code and telephone number of the security monitor.

FAX . . . . Enter the area code and fax number of the security monitor.

E-MAIL . . . . Enter the e-mail address of the security monitor.

ADDRESS . . . . Enter the address of the LDSS/AGENCY.

CITY,STATE,ZIP . . . . Enter the city, state, and zip code of the LDSS/AGENCY

JOB CLASSIFICATION . . . . Enter the job classification of the security monitor.

JOB TITLE . . . . Enter the title of the security monitor.

STATE EMPLOYEE: . . . . Check the appropriate box.

IF NO EXPLAIN: . . . . If the logonid request is not for a state employee supply justification for the logonid.

APPOINTING AUTHORITY

TITLE . . . . Enter the appointing authority's title.

NAME . . . . Enter the name of the appointing authority..

(FIRST) - enter first name here
(LAST) - enter last name here

DATE: . . . . Enter the date the signature below was added.

SIGNATURE . . . . Enter the signature of the appointing authority.

PHONE . . . . Enter the area code and telephone of the appointing authority.

FAX . . . . Enter the area code and fax number of the appointing authority.

E-MAIL . . . . Enter the e-mail address of the appointing authority.

ADDRESS . . . . Enter the address of the LDSS/AGENCY of the appointing authority.

CITY,STATE,ZIP . . . . Enter the city, state, and the zip code of the LDSS/AGENCY of the appointing authority.

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
PROCEDURE FOR COMPLETING DATA SECURITY ACCESS FORMS

FORM NUMBER: DHR/OIM 672 (02/03) **ISSUED: 14FEB03** **REVISED:** **PAGE 1 OF 2**

USAGE: Used to grant access to the CARES/SERVICES automated systems.

PROCEDURE: The supervisor completes and signs the DHR/OIM 672 and submits it to the security monitor. The local security monitor authorizes the request(s) and submits the signed form(s) to the DHR/OIM Data Security Division.

NOTE: A logonid and/or services workerid must be established prior to the submission of or with this request.

INSTRUCTIONS FOR COMPLETING THE FORM:

ACTION: .... Check one box per request:

ADD	- to establish access
UPDATE	- to change the employee's access privileges or to modify their information
SUSPEND	- to temporarily disable access in CARES or SERVICES

DATE OF REQUEST: .... Enter the current date.

CURRENT LOGONID: .... Enter the employee's logonid. (THIS IS REQUIRED FOR UPDATE and DELETE).

EMPLOYEE NAME (PRINT): .... Enter the name of the employee.

(FIRST)	- enter first name here
(LAST)	- enter last name here

LDSS: .... Enter the LDSS or agency location name. Refer to Appendix B.

PHONE: .... Enter the area code and telephone number of the employee.

JOB CLASSIFICATION: .... Enter the job classification of the employee. (THIS IS REQUIRED FOR ADD and UPDATE)

DISTRICT: .... Enter the local department's district location name, if applicable.

LOCATION CODE: .... Refer to Appendix B. (2 DIGIT CODE ONLY).

STATE EMPLOYEE: .... Check the appropriate box.

IF NO EXPLAIN: .... If the logonid request is not for a state employee supply justification for the logonid.

NOTICE NAME .... Enter the employee's name as it will appear on the CARES client notices. Maximum of 25 characters.

USER'S SYSTEM .... Check the appropriate Boxes per request. Access can be granted for CARES **or** SERVICES.

NON PRODUCTION CICS REGION(S) .... Enter information as required.

CARES

WORKER TYPE .... Enter the letter "P" for a probationary worker, a letter "S" for a supervisor, otherwise leave blank (Refer to Appendix H).

UNIT TYPE .... Enter the two digit unit type. (Refer to Appendix F).

UNIT NUMBER .... Enter a two character number indicating the supervisory group to which the employee belongs. (Refer to Appendix C).

INSTRUCTIONS FOR COMPLETING THE FORM (CONTINUED) :

DISTRICT OFFICE .... Enter the local department's three character district code. (Refer to Appendix C).

LDSS ACCESS .... Used for multiple office jurisdictions to grant access to cases in any of those offices. Enter a "Y" if access is required. Enter a "N" or leave blank if access is not required.

SERVICES

WORKER TYPE .... Enter the two character worker type. (Refer to Appendix H).

FACTS WORKER TYPE .... Enter the one character FACTS worker type. This is required for Unit Types 35 and 37 only. (Refer to Appendix I).

WORKER ID .... Enter the worker Identification code for a services employee who is not requesting logon access to the SERVICES data base.

UNIT TYPE .... Enter the two character unit type. (Refer to Appendix F).

UNIT NUMBER .... Enter the two digit unit number which defines the supervisisory group to which the employee is assigned. (Refer to Appendix E).

DISTRICT OFFICE .... Enter the three character district office number. (Refer to Appendix C).

SECURED TASKS

DELETE SECURED TASKS ... Specify the CARES secured tasks that the user will not be authorized to access based on the chosen unit type. (Refer to Appendix J).

ADD SECURED TASK .... Specify the CARES secured tasks that the user will have added to the chosen unit type. (Refer to Appendix J).

SUPERVISOR

SIGNATURE .... Enter the signature of the supervisor of the employee noted.

DATE: .... Enter the date the above signature was added.

NAME (PRINT): .... Enter the first and last name of the supervisor of the employee noted.

PHONE: .... Enter the area code and telephone number of the security

SECURITY MONITOR

SIGNATURE .... Enter the signature of the security monitor.

DATE: .... Enter the date the above signature was added.

FAX: .... Enter the area code and facsimile number of the security monitor.

NAME (PRINT): .... Enter the first and last name of the security monitor.

PHONE: .... Enter the area code and telephone number of the security monitor.

STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES
OFFICE OF TECHNOLOGY FOR HUMAN SERVICES
PROCEDURE FOR COMPLETING DATA SECURITY ACCESS FORMS

FORM NUMBER: DHR/OIM 672b (02/03) **ISSUED:** 14FEB03 **REVISED:** PAGE 1 OF 2

USAGE: Used to grant access to the CSES automated system.

PROCEDURE: The supervisor completes and signs the DHR/OIM 672b and submits it to the security monitor. The local security monitor authorizes the request(s) and submits the signed form(s) to the DHR/OIM Data Security Division.

NOTE: A logonid must be established prior to the submission of or with this request

INSTRUCTIONS FOR COMPLETING THE FORM:

ACTION: .... Check one box per request:

ADD - to establish access
UPDATE - to change the employee's access privileges or to modify their information
DELETE - to remove the logonid from CSES

DATE OF REQUEST: .... Enter the current date.

CURRENT LOGONID: .... Enter the employee's logonid. (THIS IS REQUIRED FOR UPDATE and DELETE).

EMPLOYEE NAME (PRINT): .... Enter the name of the employee.

(FIRST) - enter first name here
(LAST) - enter last name here

LDSS: .... Enter the LDSS or agency location name. Refer to Appendix B.

PHONE: .... Enter the area code and telephone number of the employee.

JOB CLASSIFICATION: .... Enter the job classification of the employee. (THIS IS REQUIRED FOR ADD and UPDATE)

DISTRICT: .... Enter the local department's district location name, if applicable.

LOCATION CODE: .... Refer to Appendix B. (2 DIGIT CODE ONLY).

STATE EMPLOYEE: .... Check the appropriate box.

IF NO EXPLAIN: .... If the logonid request is not for a state employee supply justification for the logonid.

NON PRODUCTION CICS
REGION(S) .... Enter information as required.

EXISTING ROLE(S): .... List any roles that were granted on previous request forms.
These roles should be checked for conflicts prior to submission. (Refer to Appendix D)

DELETE ROLE(S): .... List any existing roles that are requested to be deleted by this submission.(Refer to Appendix D)

ADD ROLE(S): .... List any new roles that are requested to be added by this submission. (Refer to Appendix D)
This is for initial access requests and requests to modify existing profiles.
For the initial submission, there should be no existing roles.
For subsequent modifications of existing profiles, existing roles MUST be listed.

INSTRUCTIONS FOR COMPLETING THE FORM (CONTINUED) :

COUNTY .... Enter the two character county jurisdictional designator. (Refer to Appendix G).

AGENCY LEVEL .... Enter the one character agency level code. (Refer to Appendix G).

SECURITY LEVEL .... Enter the one character security level code. (Refer to Appendix G).

UNIT TYPE .... Pre-filled with '60'.

UNIT NUMBER .... Pre-filled with '60'.

DISTRICT OFFICE .... Pre-filled with '002'.

JUSTIFICATION .... Enter the specific job duties that require either a higher level profile than the employee's classification warrants, or detailed information as to why conflicting roles are being requested. This justification should be submitted by the Local Director, and must be approved by the Executive Director of the CSEA.

LOCAL DIRECTOR .... Signature required with justification.

EXECUTIVE DIRECTOR, CSEA Signature required with justification.

SUPERVISOR

SIGNATURE .... Enter the signature of the supervisor of the employee noted.

DATE: .... Enter the date the above signature was added.

NAME (PRINT): .... Enter the first and last name of the supervisor of the employee noted.

PHONE: .... Enter the area code and telephone number of the security

SECURITY MONITOR

SIGNATURE .... Enter the signature of the security monitor.

DATE: .... Enter the date the above signature was added.

FAX: .... Enter the area code and facsimile number of the security monitor.

NAME (PRINT): .... Enter the first and last name of the security monitor.

PHONE: .... Enter the area code and telephone number of the security monitor.